UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/598,832	09/13/2006	Dimitri Korobkov	59375.00017	1975

30256 7590 03/30/2010

SQUIRE, SANDERS & DEMPSEY L.L.P
PATENT DEPARTMENT
ONE MARITIME PLAZA, SUITE 300
SAN FRANCISCO, CA 94111-3492

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/30/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/598,832	KOROBKOV, DIMITRI	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26,28 and 29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26,28 and 29* is/are rejected.

7)☒ Claim(s) *1,4,9-13,21 and 23-25* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 September 2006* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/13/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Preliminary Amendment, received on 13 September 2006, has been entered into record. In this amendment, claims 2-12, 14-25, 28, and 29 have been amended, and claim 27 has been canceled.

2. Claims 1-26, 28, and 29 are presented for examination.

Priority

3. The claim for priority from PCT/EP05/54004 filed on 15 August 2005 is duly noted.

4. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Specification

5. The abstract of the disclosure is objected to because "(Figure 5)" after line 10 should be deleted. Correction is required. See MPEP § 608.01(b).

6. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Claim Objections

7. Claims 1, 4, 9-13, 21, and 23-25 are objected to because of the following informalities:

a. In claim 1, line 5: "a storage medium" is unclear if it relates to "storage medium" (claim 1, line 4) and should read –the storage medium–;

b. In claim 1, line 9: “the digital data stream” lacks antecedent basis;

c. In claim 1, line 10: “at least one address" is unclear if it relates to "an address" (claim 1, line 7);

d. In claim 4, line 2: “the mobile terminal" lacks antecedent basis;

e. In claim 9, line 2: “the status” lacks antecedent basis;

f. In claim 9, line 2: ‘the random generator” should read –the first random generator–;

g. In claim 10, line 3: “the access" lacks antecedent basis;

h. In claim 10, line 4: “the concrete address” lacks antecedent basis;

i. In claim 11, line 2: “the digital data” is unclear if it relates to “digital information” (claim 1, line 1);

j. In claim 12, line 2: “the noise" lacks antecedent basis;

k. In claim 13, line 1: "A communication device which encrypts a digital data stream" should read –A communication device which encrypts a digital data stream, the communication device comprising:–;

l. In claim 13, line 2: "having an interface" should read –an interface–;

m. In claim 13, line 6: “having an encryption unit” should read –an encryption unit–;

n. In claim 21, line 2: “the status" lacks antecedent basis;

o. In claim 21, line 2: "the random generator" should read –the first random generator–;

p. In claim 23, line 3: "the access" lacks antecedent basis;

q. In claim 23, line 4: "the concrete addresses" lacks antecedent basis;

r. In claim 24, lines 1-2: “The communication device claim 13” should read – The communication device according to claim 13–;

s. In claim 25, line 3: “the noise” lacks antecedent basis.

Appropriate correction is required.

8. It is noted that the claims contain dashes, which are non-functional. The examiner requests that these be removed.

Drawings

9. Figures 1a, 1b, 1c, and 4a should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled “Replacement Sheet” in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 4, 10, and 26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 4 recites the limitation "the mobile terminal" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim 10 recites the limitation “the concrete addresses of the segments” in line 4. There is insufficient antecedent basis for this limitation in the claim.

Regarding claim 26, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d). It is noted that claim 26, line 1 recites “a mobile addressed memory element, such as a flash card," which is indefinite.

Claim Rejections - 35 USC § 101

12. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-12, 26, and 28 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-12 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory “process” under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2d 1385. The instant

claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The encrypting method including steps of using is broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent. For example, using communication devices can be performed by a person.

Claim 26 is rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. Claim 26 recites “A use of a mobile addressed memory element,” which is not a process, machine, manufacture, or composition of matter. Therefore, claim 26 is directed to non-statutory subject matter.

Claim 28 is rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. Claim 28 recites “A data carrier for a computer" which typically covers forms of non-transitory tangible media and transitory propagating signals *per se*. Therefore, since a transitory propagating signal is non-statutory subject matter, claim 28 is directed to non-statutory subject matter. It is noted that if the limitation "non-transitory" were added to the claim, the data carrier of the claim would be considered statutory.

Claim Rejections - 35 USC § 102

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

14. Claims 1, 2, 4, 5, 11, 13, 14, 16, 17, 24, 26, 28, and 29 are rejected under 35 U.S.C. 102(b) as being anticipated by Bush (US 2002/0002675 A1).

As to claim 1, Bush discloses a system and method for secure encryption of data packets for transmission over unsecured networks, the system and method having:

using communication devices which have an interface for a replaceable or writable storage medium, whose content may be read out and duplicated (0032, lines 3-5),

using a storage medium which is connected to the interface, a supply of symbols for encryption being stored on the digital storage medium which may be read out on the basis of an address (0032, lines 3-5; 0061, lines 1-6),

using an encryption unit which employs the supply of symbols for encrypting or decrypting the digital data stream of the communication devices on the basis of at least one address (0041, lines 4-9; 0042, lines 3-12).

As to claim 13, Bush discloses:

having an interface for a replaceable or writable storage medium, whose content may be read out and duplicated, a supply of symbols for encryption, which may be read by using an address, being stored on the

storage medium, which may be connected to the interface (0032, lines 3-5; 0061, lines 1-6)**,**

having an encryption unit, which is set up so that it uses the supply of symbols for encrypting or decrypting the digital data stream of the communication devices by accessing this supply through addresses (0041, lines 4-9; 0042, lines 3-12)**.**

As to claims 2 and 14, Bush discloses:

wherein the symbols on the storage medium are only used once and are thus "used up" (0013, lines 8-10)**.**

As to claims 4 and 16, Bush discloses:

wherein the mobile terminal comprises one or more of the following: a radio device, laptop, PDA, a mobile telephone having an interface for a memory card that is insensitive and may be used in portable communication devices (0013, lines 12-15)**.**

As to claims 5 and 17, Bush discloses:

wherein the storage medium is one or more of the following: a flash memory card, a hard drive, an optical storage drive, whose information may be addressed (0013, lines 17-18)**.**

As to claims 11 and 24, Bush discloses:

wherein a permutation of the digital data is performed before it is transmitted (0044, lines 4-6).

As to claim 26, Bush discloses:

A use of a mobile addressed memory element, such as a flash card, which is readable by a mobile communication device, for storing symbols for encryption, the symbols being able to be addressed (0032, lines 3-5; 0061, lines 1-6).

As to claim 28, Bush discloses:

a data structure for storing instructions for a computer for executing the method according to claim 1 (0070, lines 1-5).

As to claim 29, Bush discloses:

a device which allows the execution of a method according to method claim 1 (0069, lines 1-4).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claims 3, 6-9, 15, and 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bush as applied to claims 1 and 13 above, and in view of Kauffman et al. (US 2002/0159588 A1 and Kauffman hereinafter).

As to claims 3 and 15, Bush fails to specifically disclose:

wherein the symbols are encrypted and decrypted with the data stream using mod2.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush, as taught by Kauffman.

Kauffman discloses a system and method for cryptography with unconditional security, the system and method having:

wherein the symbols are encrypted and decrypted with the data stream using mod2 (0004, lines 1-9)**.**

Given the teaching of Kauffman, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush with the teachings of Kauffman by using mod2 for encryption and decryption. Kauffman recites motivation by disclosing that using modulo 2 for encryption reduces the data size of the resulting cryptogram (0004, lines 1-3). It is obvious that the teachings of Kauffman would have improved the teachings of Bush by using mod2 for encryption and decryption in order to produce a cryptogram that is smaller in size.

As to claims 6 and 18, Bush fails to specifically disclose:

wherein the addresses of the symbols to be used on the storage medium are transmitted to synchronize the encryption.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush, as taught by Kauffman.

Kauffman discloses:

wherein the addresses of the symbols to be used on the storage medium are transmitted to synchronize the encryption (0006, lines 6-10)**.**

Given the teaching of Kauffman, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush with the teachings of Kauffman by transmitting information for synchronizing the symbols. Kauffman recites motivation by disclosing that the receiver must have the same random number sequence the sender used or must be able to reproduce it in order to perform successful encryption and decryption (0005, lines 3-5). It is obvious that the teachings of Kauffman would have improved the teachings of Bush by transmitting information for synchronizing the symbols in order to ensure that the sender and receiver are using the same sequence.

As to claims 7 and 19, Bush fails to specifically disclose:

wherein the addresses are transmitted at specific intervals to synchronize the encryption.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush, as taught by Kauffman.

Kauffman discloses:

> **wherein the addresses are transmitted at specific intervals to synchronize the encryption** (0021, lines 11-15)**.**

Given the teaching of Kauffman, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush with the teachings of Kauffman by transmitting information for synchronization at specific intervals. Kauffman recites motivation by disclosing that synchronizing at regular intervals thwarts attackers from attacking the random generator's state (0021, lines 13-14) while ensuring that the sender and receiver are using the same sequence (0005, lines 3-5). It is obvious that the teachings of Kauffman would have improved the teachings of Bush by transmitting synchronization information at specific intervals in order to prevent attackers from attacking a generator's state while ensuring that successful encryption and decryption can be performed.

As to claims 8 and 20, Bush fails to specifically disclose:

> **wherein there is a first random generator (PRG2) on the communication device which determines the address on the storage medium.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush, as taught by Kauffman.

Kauffman discloses:

> **wherein there is a first random generator (PRG2) on the communication device which determines the address on the storage medium** (0013, lines 8-14)**.**

Given the teaching of Kauffman, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush with the teachings of Kauffman by randomly determining an address. Kauffman recites motivation by disclosing that combining a pseudorandom number generator and an encoding algorithm produces an unbreakable cryptographic scheme for communications and data storage (0007, lines 2-4). It is obvious that the teachings of Kauffman would have improved the teachings of Bush by randomly determining an address in order to produce an unbreakable cryptographic scheme.

As to claims 9 and 21, Bush fails to specifically disclose:

> **wherein the status of the random generator is transmitted to synchronize the encryption.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush, as taught by Kauffman.

Kauffman discloses:

wherein the status of the random generator is transmitted to synchronize the encryption (0031, lines 10-15)**.**

Given the teaching of Kauffman, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush with the teachings of Kauffman by transmitting the status of a generator for synchronization. Please refer to the motivation recited above with respect to claims 6 and 18 as to why it is obvious to apply the teachings of Kauffman to the teachings of Bush.

As to claim 22, Bush fails to specifically disclose:

means, through which the status of the random generator is transmitted at specific intervals.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush, as taught by Kauffman.

Kauffman discloses:

means, through which the status of the random generator is transmitted at specific intervals (0021, lines 11-15)**.**

Given the teaching of Kauffman, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush with the teachings of Kauffman by transmitting the status of a generator at specific intervals. Please refer to the motivation recited above

with respect to claims 7 and 19 as to why it is obvious to apply the teachings of Kauffman to the teachings of Bush.

17. Claims 10 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bush in view of Kauffman as applied to claims 8 and 20 above, and further in view of Glover (US 6,868,495 B1).

As to claims 10 and 23, Bush in view of Kauffman fail to specifically disclose:

> **wherein there is a second random generator (PRG1) which performs scrambling of the access to individual segments if PRG2 determines the concrete addresses of the segments.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush in view of Kauffman, as taught by Glover.

Glover discloses a system and method for one-time pad encryption key distribution, the system and method having:

> **wherein there is a second random generator (PRG1) which performs scrambling of the access to individual segments if PRG2 determines the concrete addresses of the segments** (col. 22, lines 51-56)**.**

Given the teaching of Glover, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush in view of Kauffman with the teachings of Glover by scrambling access to symbols. Glover recites motivation by disclosing that changing parameters

and decrypting code helps to thwart the efforts of a brute force attack (col. 22, lines 66-67; col. 23, line 1). It is obvious that the teachings of Glover would have improved the teachings of Bush in view of Kauffman by scrambling access to symbols in order to prevent brute force attacks.

18. Claims 12 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bush as applied to claims 1 and 13 above, and in view of Shefi (US 6,445,794 B1).

wherein the storage medium is written by the noise of an analog source using an A/D converter.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Bush, as taught by Shefi.

Shefi discloses a system and method for synchronizing one time pad encryption keys, the system and method having:

wherein the storage medium is written by the noise of an analog source (col. 4, lines 58-64) but does not disclose the usage of an A/D converter.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to use an A/D converter to convert an analog signal to a digital signal since it was known in the art that an analog noise signal must be converted before it can be used in a digital system.

Given the teaching of Shefi, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Bush with the teachings of Shefi by using an analog noise source.

Shefi recites motivation by disclosing that using a source of physical random phenomena can produce true random numbers (col. 4, lines 58-60). It is obvious that the teachings of Shefi would have improved the teachings of Bush by using an analog noise source in order to produce true random numbers.

Prior Art Made of Record

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Spacey (US 2003/0048899 A1) discloses a system and method for securing electronic information.

b. Hattick et al. (US 2003/0112972 A1) discloses a system and method for secure transmission of information.

c. Finn et al. (US Patent 5,940,002) discloses a system and method for random number remote communications.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431

/Sarah Su/
Examiner, Art Unit 2431